

**IN THE CLAIMS:**

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~striketrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please CANCEL claims 5, 10 and 11; AMEND claims 1, 6-9, 12-16, 18-19 and 24-29 and ADD claims 30-33 in accordance with the following:

1. (currently amended) A signature system presenting a receiver with signature information of a user, comprising:
  - an input unit inputting ~~the~~ identification information of the user; and
  - an output unit outputting information for generation of the signature information according to the input identification information, the output information including program information for generation of illegal use prevention information for protection against illegal use in a format readable by a bar cord reader.
2. (original) The system according to claim 1, wherein said output unit encrypts and outputs the identification information.
3. (original) The system according to claim 1, wherein said input unit inputs authentication information, which is significant and repeatedly reproducible by the user, as the identification information.
4. (original) The system according to claim 1, wherein said input unit inputs image data of an image of a seal as the identification information.
5. (cancelled)
6. (currently amended) The system according to claim-~~5~~1, wherein said program information contains a one-directional function, and is used in generating blind information of use information using the one-directional function, and generating the illegal use prevention information containing the blind information.

7. (currently amended) The system according to claim-5\_1, wherein said program information contains an encryption key, and is used in generating blind information of use information using the encryption key, and generating the illegal use prevention information containing the blind information.

8. (currently amended) The system according to claim-5\_1, wherein said program information is prepared such that, after the signature information is generated according to the information for generation of the signature information to present the signature information to the receiver, the program information itself can be removed from memory.

9. (currently amended) A signature system presenting signature information of a user to a receiver, comprising:

a reading unit reading information, including program information, for generation of the signature information in a bar code format; and

a generation unit generating the signature information and illegal use prevention information for protection against illegal use according to the read information.

10. (cancelled)

11. (cancelled)

12. (currently amended) The system according to claim-40\_32, further comprising[[:]] a timer unit generating date and time information used as the illegal use prevention information.

13. (currently amended) The system according to claim 9, further comprising:

a management unit managing first blind information of identification information contained in the read information ~~in the bar code format~~; and

a comparison unit generating second blind information of the identification information from use information contained in the signature information, and comparing the ~~obtained second~~ blind information with the first blind information ~~managed by said management unit~~.

14. (currently amended) The system according to claim ~~43~~ 19, further comprising an issue unit issuing certification information containing the blind information of the identification information.

15. (currently amended) A signature system, comprising:  
an input unit through which a user inputs authentication information, ~~which is significant and repeatedly reproducible by the user;~~  
a first generation unit generating first blind information of the authentication information; and  
~~an entry unit entering the blind information in a device verifying signature information according to the authentication information, including an entry unit entering the blind information; and~~  
a management unit managing the blind information of the authentication information entered by said entry unit.

16. (currently amended) The system according to claim 15,  
wherein said entry unit enters in the device verifying the signature a one-directional function and an encryption key, which are used to generate the blind information and required to authenticate a user, and  
wherein said management unit further manages the one-directional function and the encryption key entered by said entry unit.

17. (original) The system according to claim 15, wherein said input unit and said generation unit are provided in a terminal of the user.

18. (currently amended) The system according to claim 15, wherein when said user ~~presents the signature information to a receiver for authentication, said user re-enters the authentication information through said input unit, and said generation unit generates the signature information from~~ encrypts the re-entered authentication information.

19. (currently amended) The system according to claim 18, further comprising:  
a second generation unit newly generating second blind information from the re-entered authentication information using a one-directional function and an encryption key entered in the device verifying the signature information managed by said management unit; and

a comparison unit reading the first blind information entered in the device, and comparing the first blind information with the ~~newly generated~~ second blind information.

20. (original) The system according to claim 19, further comprising a deletion unit removing the re-entered authentication information from memory after the newly generated blind information is compared with the blind information entered in the device.

21. (original) The system according to claim 15, wherein said input unit selectively inputs the authentication information from among a plurality of items in an interactive mode with said user.

22. (original) The system according to claim 21, wherein said input unit changes the number of input items of the authentication information depending on a usage of the signature information.

23. (original) The system according to claim 15, wherein after entering the blind information, said entry unit removes the authentication information based on which the blind information is generated in order to avoid an illegal use by others.

24. (currently amended) A computer-readable storage medium storing a program used to direct a computer to perform a method comprising:

inputting identification information of a user;

generating information for generation of signature information of the user according to the input identification information;

generating a signature program for generation of illegal use prevention information; and

outputting the generated information and the signature program in a format readable by a bar code reader.

25. (currently amended) A computer-readable storage medium storing a program used to direct a computer to perform a method comprising:

reading information in a bar code format, including program information, for generation of signature information; and

generating the signature information of a user and illegal use prevention information for protection against illegal use, based on the read information.

26. (currently amended) A computer-readable storage medium storing a program used to direct a computer to perform a method comprising:

~~inputting~~ managing first blind information generated from authentication information, which is significant and repeatedly reproducible a one-directional function and an encryption key which are registered by a user;

~~generating~~ second blind information of the from re-entered authentication information using the one-directional function and encryption key; and

~~entering~~ comparing the first blind information in a device verifying signature information according to the authentication with the second blind information.

27. (currently amended) A signature system presenting a receiver with signature information of a user, comprising:

input means for inputting the identification information of the user; and

output means for outputting information for generation of the signature information according to the input identification information in a format readable by a bar code reader and for generating a signature program for generation of illegal use prevention information.

28. (currently amended) A signature system presenting signature information of a user to a receiver, comprising:

reading means for reading information in a bar code format, including program information, for generation of the signature information; and

generation means for generating the signature information and illegal use prevention information for protection against illegal use according to the read information.

29. (currently amended) A signature system, comprising:

~~input management~~ means through which a user inputs first blind information generated from authentication information, which is significant and repeatedly reproducible a one-directional function and an encryption key which are registered by the user;

generation means for generating ~~second~~ blind information of the from re-entered authentication information using the one-directional function and encryption key; and

~~entry-comparison~~ means for ~~entering-comparing~~ the first blind information in a device ~~verifying signature information according to the authentication with the second blind~~ information.

30. (new) The signature system according to claim 1, wherein said output unit outputs the information for generation of the signature information in a format readable by a bar code reader.

31. (new) The signature system according to claim 9, wherein said reading unit reads the program information in a bar code format.

32. (new) The signature system according to claim 9,  
wherein said program information contains a one-directional function and an encryption key, and  
wherein said generation unit generates blind information from use information using the one-directional function and the encryption key, generates the signature information by attaching to read information the blind information and the use information, and generates the illegal use prevention information containing the blind information.

33. (new) The signature system according to claim 9, wherein said program information can be removed from memory after the signature information is generated according to the information for generation of the signature information.